Cyber Security: Machine Learning and Big Data Know It Wasn't You Who Just Swiped Your Credit Card

You're sitting at home minding your own business when you get a call from your credit card's fraud detection unit asking if you've just made a purchase at a department store in your city. It wasn't you who bought expensive electronics using your credit card – in fact, it's been in your pocket all afternoon. So how did the bank know to flag this single purchase as most likely fraudulent?

Credit card companies have a vested interest in identifying financial transactions that are illegitimate and criminal in nature. The stakes are high. According to the Federal Reserve Payments Study, Americans used credit cards to pay for 26.2 billion purchases in 2012. The estimated loss due to unauthorized transactions that year was US$6.1 billion. The federal Fair Credit Billing Act limits the maximum liability of a credit card owner to $50 for unauthorized transactions, leaving credit card companies on the hook for the balance. Obviously fraudulent payments can have a big effect on the companies'

bottom lines. The industry requires any vendors that process credit cards to go through security audits every year. But that doesn't stop all fraud.

In the banking industry, measuring risk is critical. The overall goal is to figure out what's fraudulent and what's not as quickly as possible, before too much financial damage has been done. So how does it all work? And who's winning in the arms race between the thieves and the financial institutions?

Gathering the troops

From the consumer perspective, fraud detection can seem magical. The process appears instantaneous, with no human beings in sight. This apparently seamless and instant action involves a number of sophisticated technologies in areas ranging from finance and economics to law to information sciences.

Of course, there are some relatively straightforward and simple detection mechanisms that don't require advanced reasoning. For example, one good indicator of fraud can be an inability to provide the correct zip code affiliated with a credit card when it's used at an unusual location. But fraudsters are adept at bypassing this kind of routine check – after all, finding out a victim's zip code could be as simple as doing a Google search.

Traditionally, detecting fraud relied on data analysis techniques that required significant human involvement. An algorithm would flag suspicious cases to be closely reviewed ultimately by human investigators who may even have called the affected cardholders to ask if they'd actually made the charges. Nowadays the companies are dealing with a constant deluge of so many transactions that they need to rely on big data analytics for help. Emerging technologies such as machine learning and cloud computing are stepping up the detection game.